Wireshark Developer and User Conference

B-1: I've Just Downloaded Wireshark… Now What?

Tuesday June 14, 2011 - 10:15am - 11:30am

Betty DuBois
Principal Consultant | DuBois Training & Consultant, LLC
Betty@DTCpackets.com

SHARKFEST '11
Stanford University
June 13-16, 2011

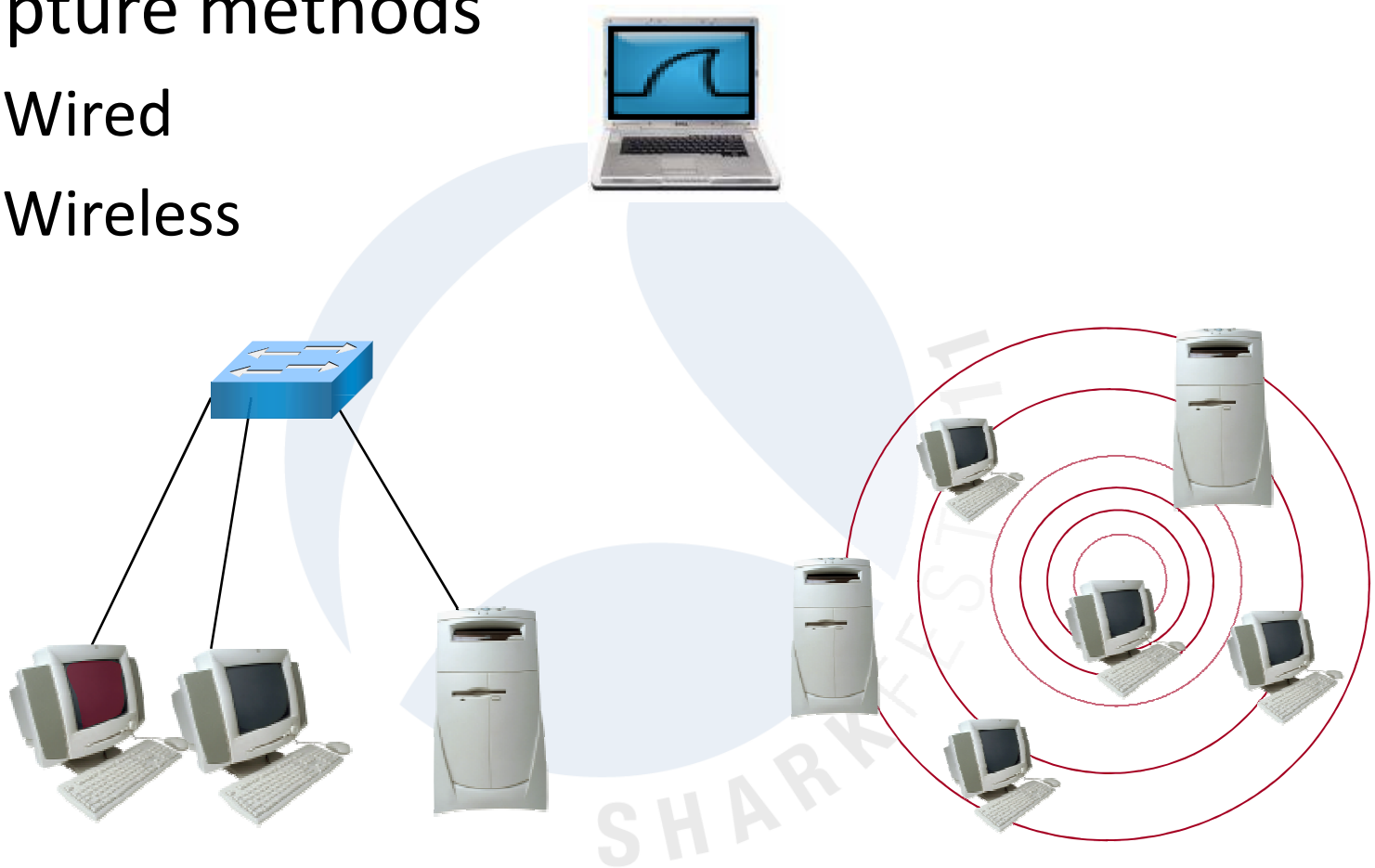
Agenda

- Data Capture
  - Capture methods
    - Caveats
  - Capture interfaces

- Data Analysis
  - Statistics
    - Summary Information
    - Protocol hierarchy
    - Conversations
    - Endpoints
  - Basic display filtering
  - Reassembly
  - Coloring rules

Data Capture – How do I get the data?

- Capture methods
  - Wired
  - Wireless

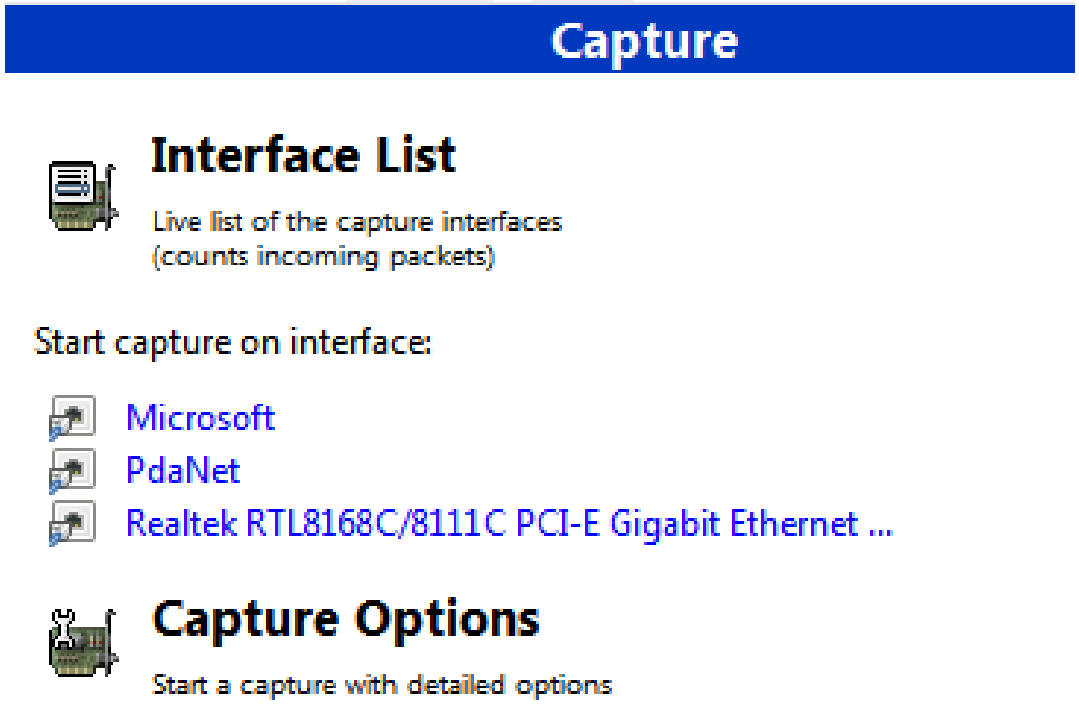


Data Capture – How do I get the data?

- Capture Caveats
  - Wired
    - Mirrors/Monitors/SPANs
    - Taps
    - Hubs
  - Wireless
    - Promiscuous vs. rfmon/monitor mode
    - AirPcap

Data Capture - Options

- Which interface to use?
- What about permissions?



Data Analysis

- Don’ts
  - Don’t get caught in the vortex!
  - Don’t start by scrolling through the packets
- Do’s
  - Use Statistics to baseline your environment
  - Use Statistics to determine where your focus should be
  - Use filtering to focus

Data Analysis – Statistics > Protocol Hierarchy

Wireshark: Protocol Hierarchy Statistics

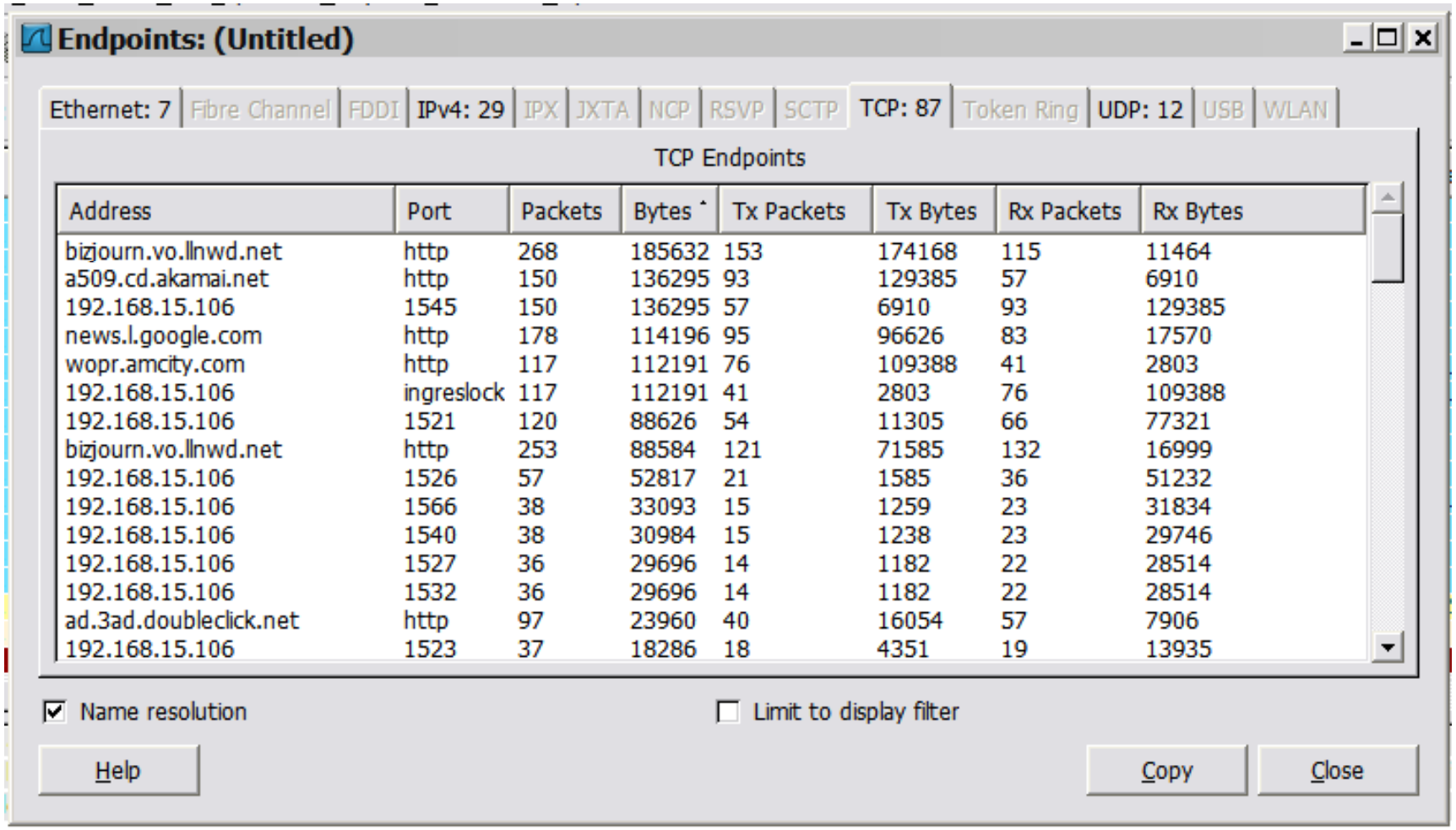
Display filter: none

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100.00%	1245	708592	0.071	0	0	0.000
Ethernet	100.00%	1245	708592	0.071	0	0	0.000
Address Resolution Protocol	0.16%	2	102	0.000	2	102	0.000
Internet Protocol	99.84%	1243	708490	0.071	0	0	0.000
User Datagram Protocol	3.05%	38	4479	0.000	0	0	0.000
Domain Name Service	2.89%	36	3976	0.000	36	3976	0.000
NetBIOS Datagram Service	0.16%	2	503	0.000	0	0	0.000
SMB (Server Message Block Protocol)	0.16%	2	503	0.000	0	0	0.000
SMB MailSlot Protocol	0.16%	2	503	0.000	0	0	0.000
Microsoft Windows Browser Protocol	0.08%	1	243	0.000	1	243	0.000
Data	0.08%	1	260	0.000	1	260	0.000
Transmission Control Protocol	96.63%	1203	703891	0.070	635	35976	0.004
Hypertext Transfer Protocol	45.22%	563	666428	0.067	477	562872	0.056
Line-based text data	2.41%	30	36903	0.004	30	36903	0.004
JPEG File Interchange Format	2.01%	25	37160	0.004	25	37160	0.004
Compuserve GIF	2.17%	27	25363	0.003	20	14765	0.001
Unreassembled Fragmented Packet	0.56%	7	10598	0.001	7	10598	0.001
Media Type	0.24%	3	3664	0.000	3	3664	0.000
eXtensible Markup Language	0.08%	1	466	0.000	1	466	0.000
Secure Socket Layer	0.40%	5	1487	0.000	3	511	0.000

Help Close

Data Analysis – Statistics > End Points

- Add GeoIP info - Instructions on wiki.wireshark.org



Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
bizjourn.vo.llnwd.net	http	268	185632	153	174168	115	11464
a509.cd.akamai.net	http	150	136295	93	129385	57	6910
192.168.15.106	1545	150	136295	57	6910	93	129385
news.l.google.com	http	178	114196	95	96626	83	17570
wopr.amcity.com	http	117	112191	76	109388	41	2803
192.168.15.106	ingreslock	117	112191	41	2803	76	109388
192.168.15.106	1521	120	88626	54	11305	66	77321
bizjourn.vo.llnwd.net	http	253	88584	121	71585	132	16999
192.168.15.106	1526	57	52817	21	1585	36	51232
192.168.15.106	1566	38	33093	15	1259	23	31834
192.168.15.106	1540	38	30984	15	1238	23	29746
192.168.15.106	1527	36	29696	14	1182	22	28514
192.168.15.106	1532	36	29696	14	1182	22	28514
ad.3ad.doubleclick.net	http	97	23960	40	16054	57	7906
192.168.15.106	1523	37	18286	18	4351	19	13935

Data Analysis – Statistics > Conversations

Conversations: (Untitled)

Ethernet: 7 | Fibre Channel | FDDI | IPv4: 27 | IPX | JXTA | NCP | RSVP | SCTP | TCP: 67 | Token Ring | UDP: 9 | USB | WLAN

TCP Conversations

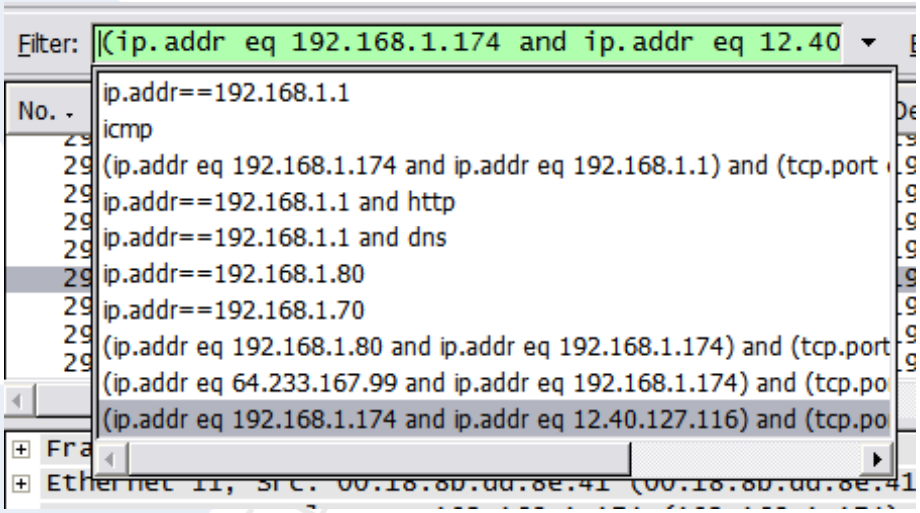
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A->B	Bytes A->B	Packets
192.168.15.106	1545	a509.cd.akamai.net	http	150	136295	57	6910	93
192.168.15.106	ingreslock	wopr.amcity.com	http	117	112191	41	2803	76
192.168.15.106	1521	news.l.google.com	http	120	88626	54	11305	66
192.168.15.106	1526	bizjourn.vo.llnwd.net	http	57	52817	21	1585	36
192.168.15.106	1566	bizjourn.vo.llnwd.net	http	38	33093	15	1259	23
192.168.15.106	1540	bizjourn.vo.llnwd.net	http	38	30984	15	1238	23
192.168.15.106	1527	bizjourn.vo.llnwd.net	http	36	29696	14	1182	22
192.168.15.106	1532	bizjourn.vo.llnwd.net	http	36	29696	14	1182	22
192.168.15.106	1523	news.l.google.com	http	37	18286	18	4351	19
192.168.15.106	1574	a1166.g.akamai.net	http	17	11329	8	1031	9
192.168.15.106	1544	bizjourn.vo.llnwd.net	http	15	8828	7	825	8
192.168.15.106	1543	bizjourn.vo.llnwd.net	http	14	8149	7	813	7
192.168.15.106	1536	w.sharethis.com	http	15	7990	7	1013	8
192.168.15.106	1535	bizjourn.vo.llnwd.net	http	15	7150	7	802	8

☑ Name resolution ☐ Limit to display filter

Help Copy Close

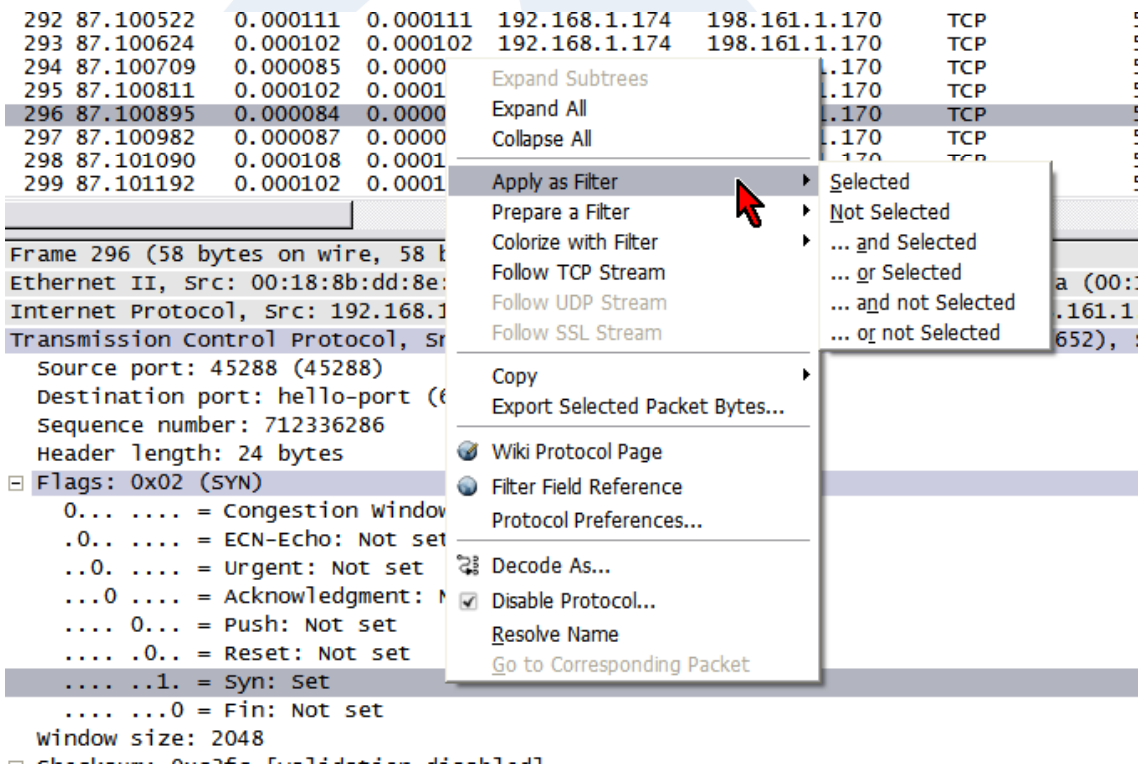
Data Analysis – Basic Display Filters

- Filter Bar – Auto-complete since 1.2
  - The Filter bar will change colors to signify if your syntax is correct
    - Green is correct
    - Red is incorrect
    - Yellow is questionable
  - The Filter dropdown will let you chose your 10 most recent filters by default
    - You can increase this in Edit>Preferences



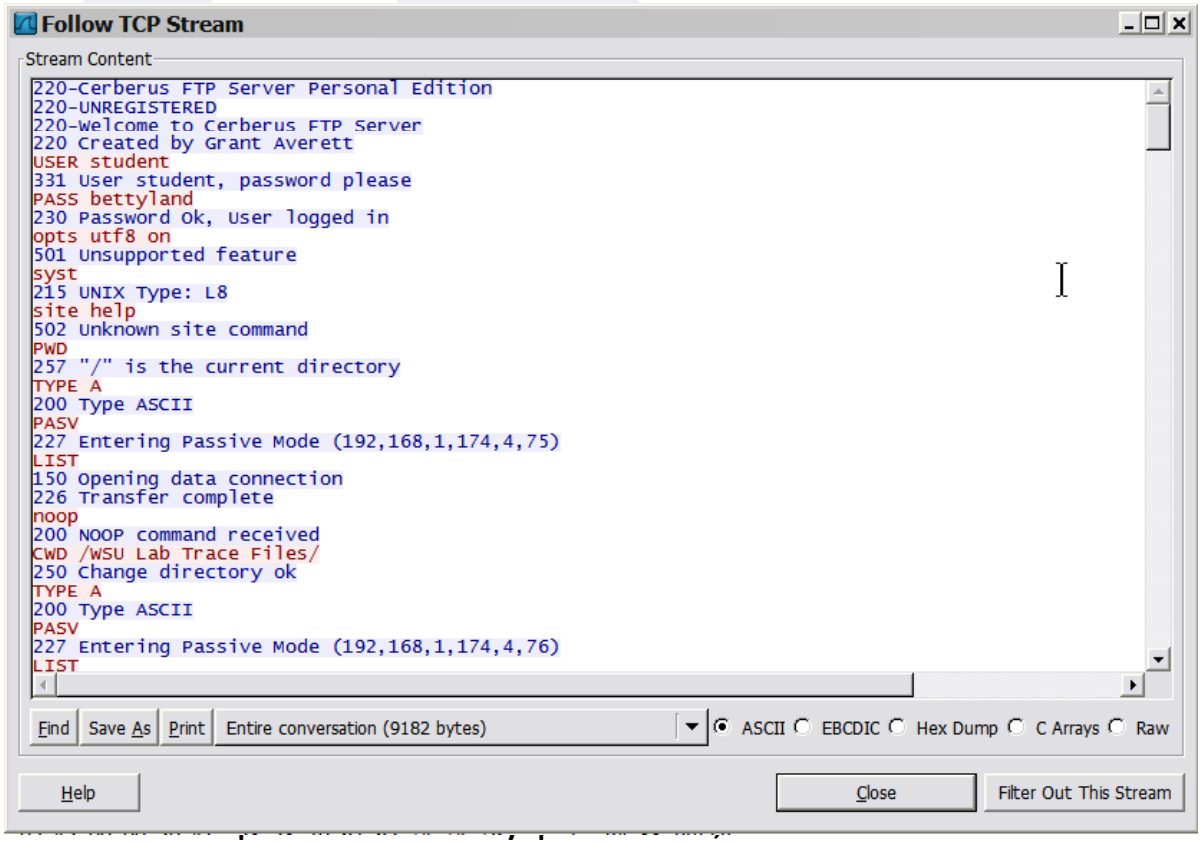
Data Analysis – Basic Display Filters

- When in doubt, right-click.
  - Find the fields you are interested in first, then build your filters with a right-click.



Data Analysis - Reassembly

- Follow the Streams – Favorite feature in Wireshark
- Available stream types:
  - TCP
  - UDP
  - SSL

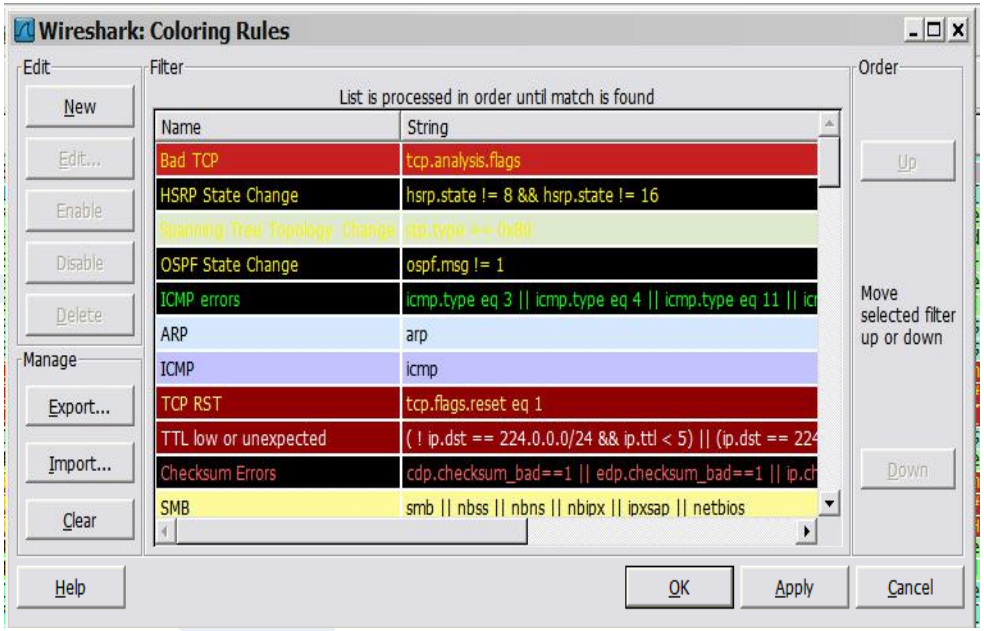


Data Analysis – Coloring Rules

- Colors help you focus on specific protocols, and/or to spot errors quickly.

Source	Destination	Protocol	Bytes	Info
192.168.1.174	167.181.46.21	SSLv3	796	Application Data
167.181.46.21	192.168.1.174	SSLv3	1158	Continuation Data, [Unreassembled Packet]
12.40.127.116	192.168.1.174	TCP	60	http > 1238 [ACK] Seq=1969644649 Ack=33526414
12.40.127.116	192.168.1.174	HTTP	147	HTTP/1.1 304 Not Modified
12.40.127.116	192.168.1.174	HTTP	156	Continuation or non-HTTP traffic
192.168.1.174	12.40.127.116	TCP	54	1238 > http [ACK] Seq=3352641413 Ack=19696448
192.168.1.174	12.40.127.116	HTTP	686	GET /assets/images/invalid.gif HTTP/1.1
192.168.1.174	167.181.46.21	TCP	54	1237 > https [ACK] Seq=1968511636 Ack=9672987
167.181.46.21	192.168.1.174	TCP	60	https > 1243 [ACK] Seq=2946753473 Ack=2624183
167.181.46.21	192.168.1.174	SSLv3	431	[TCP Previous segment lost] Continuation Data
192.168.1.174	167.181.46.21	TCP	66	[TCP Dup ACK 140678#1] 1243 > https [ACK] Seq
167.181.46.21	192.168.1.174	SSL	1462	[TCP Out-Of-Order] [Unreassembled Packet]
192.168.1.174	167.181.46.21	TCP	54	1243 > https [ACK] Seq=2624183869 Ack=2946755
12.40.127.116	192.168.1.174	TCP	60	http > 1234 [ACK] Seq=2590892468 Ack=41633224
12.40.127.116	192.168.1.174	HTTP	156	[TCP Previous segment lost] Continuation or n
192.168.1.174	12.40.127.116	TCP	54	[TCP Dup ACK 140675#1] 1234 > http [ACK] Seq=
12.40.127.116	192.168.1.174	HTTP	147	[TCP Out-Of-Order] HTTP/1.1 304 Not Modified
192.168.1.174	12.40.127.116	TCP	54	1234 > http [ACK] Seq=4163322456 Ack=25908926
192.168.1.174	12.40.127.116	HTTP	683	GET /assets/images/list.gif HTTP/1.1
167.181.46.21	192.168.1.174	SSL	1462	[Unreassembled Packet]
167.181.46.21	192.168.1.174	SSLv3	1462	Continuation Data, [Unreassembled Packet]
192.168.1.174	167.181.46.21	TCP	54	1243 > https [ACK] Seq=2624183869 Ack=2946758
167.181.46.21	192.168.1.174	SSL	1462	[Unreassembled Packet]

Data Analysis – Coloring Rules



- Rules to live by:
  - Color rules are read like an ACL
    - First rule in the list to apply wins, even if multiple rules apply
  - Rule sets can be shared among friends with Import/Export
  - Use an empty rule set if you normally use a complex rule set, but commonly turn off your colors. Your files will load faster.
  - Check out Laura's presentation on customization at 2pm today!!

Q & A

- Questions?????

Thanks For Coming!

Enjoy the rest of the conference.